DEPARTMENT OF JUSTICE
OFFICE OF JUSTICE PROGRAMS

Amber Alert Project

July 31, 2003

Amber Alert Messaging Framework

DOJ OJP Amber Alert Project

Amber Alert Messaging Framework

Prepared for:
Department of Justice
Office of Justice Programs
Office of the CIO

Prepared by:
Aquilent, Inc.
1100 West Street
Laurel, MD 20707

July 31, 2003

Table of Contents

List of Tables and Figures

Figures

1   Introduction

This document is the *Amber Alert Messaging Framework* for the DOJ Amber Alert project. The Messaging Framework is a draft description of how the Amber Alert XML specification could be used to share Amber Alert data. The actual XML schemas for the XML messages described in this document can be found in Appendix A, along with some diagrams that help to explain their structure.

1.1   Purpose

The intent of this document is to describe the proposed interactions that will be available to users of an Amber Alert Provider. These interactions consist of a sequence of two or more XML messages that will be used to communicate with the Amber Alert Provider.

1.2   Approach

The Messaging Framework and draft XML schemas were developed based on initial research conducted with various Amber Alert resources, including members of the Amber Alert working group. More detailed information describing the proposed process of how Amber Alert data could be shared across agencies, including details on the message interactions, is planned to be discussed in a separate Draft Concept of Operations document after further analysis.

The draft Amber Alert XML schemas were developed using the Justice XML Data Dictionary (JXDD) 3.0. JXDD was designed to provide a common vocabulary and set of reusable components that can enable justice and public safety organizations to build schemas rapidly, efficiently, and consistently. The draft Amber Alert XML schemas reuse JXDD components per published instructions and is implemented the same way as the RapSheet and Inmate schemas which are also based on the JXDD.

1.3   Definitions

This section describes the major users of the XML information, as described in the Message Sequence diagrams in Section 2.0.

1. Amber Alert Provider – manages the flow of data between producers and consumers of alerts.

2. Authorized Amber Alert Publisher – producers of Amber Alert data, issue and update Amber Alerts.

3. Amber Alert Notification System – facilitates the consumption of Amber Alert data.

2   Message Sequences

2.1   Amber Alert Directives

Figure 2-1 illustrates the sending of an AmberAlertDirective to the Amber Alert provider. An AmberAlertDirective is a special type of message. AmberAlertDirective messages request that the provider perform an action, such as publishing a new Amber Alert (see Figure 2-2). These actions do not require the provider to return any data to the requestor, however an AmberAlertReceipt will be returned in order to acknowledge successful receipt of the message. More information about the specific types of AmberAlertDirectives can be found below.

2.1.1   New Amber Alert

First, an AmberAlertDirective XML message is sent from an authorized publisher. This message contains the NewAmberAlert directive as well as the actual AmberAlert XML message itself. It is the included AmberAlert message that contains the actual information about the alert. The Amber Alert provider will respond with an AmberAlertReceipt XML message that serves to confirm that the alert has been successfully published to the provider. Additionally, this message contains the unique ID that was assigned to the Amber Alert.

In the case where there is an error, either due to a problem with the AmberAlertDirective itself or for some other reason, an AmberAlertReceipt XML message with a status of 'Error' is returned. The practice of sending an AmberAlertReceipt XML message with a status of 'Error' whenever a problem occurs during a sequence of messages is a standard practice that will be applied to all of the message sequences.

2.1.2   Updating an Amber Alert

The authorized publisher sends an AmberAlertDirective XML message to the Provider. This message contains an AmberAlertUpdate directive that references the Amber Alert to be updated. Contained in the AmberAlertUpdate directive is the updated Amber Alert information in the form of an AmberAlert XML message. This same procedure is used to cancel an existing Amber Alert by changing the status of the AmberAlert message to indicate that it has been cancelled.

2.1.3   Canceling an Amber Alert

The authorized publisher of the AmberAlert to be cancelled sends an AmberAlertDirective XML message to the provider containing the CancelAmberAlert directive. Within this directive is the unique ID of the Amber Alert to be canceled, as well as some indication of why the alert is being canceled.

2.1.4   Canceling a Search

A previously registered search (see Retrieving Amber Alerts) is canceled by sending the CancelSearch directive within an AmberAlertDirective XML message. The CancelSearch directive contains the name of the registered search that is to be canceled.

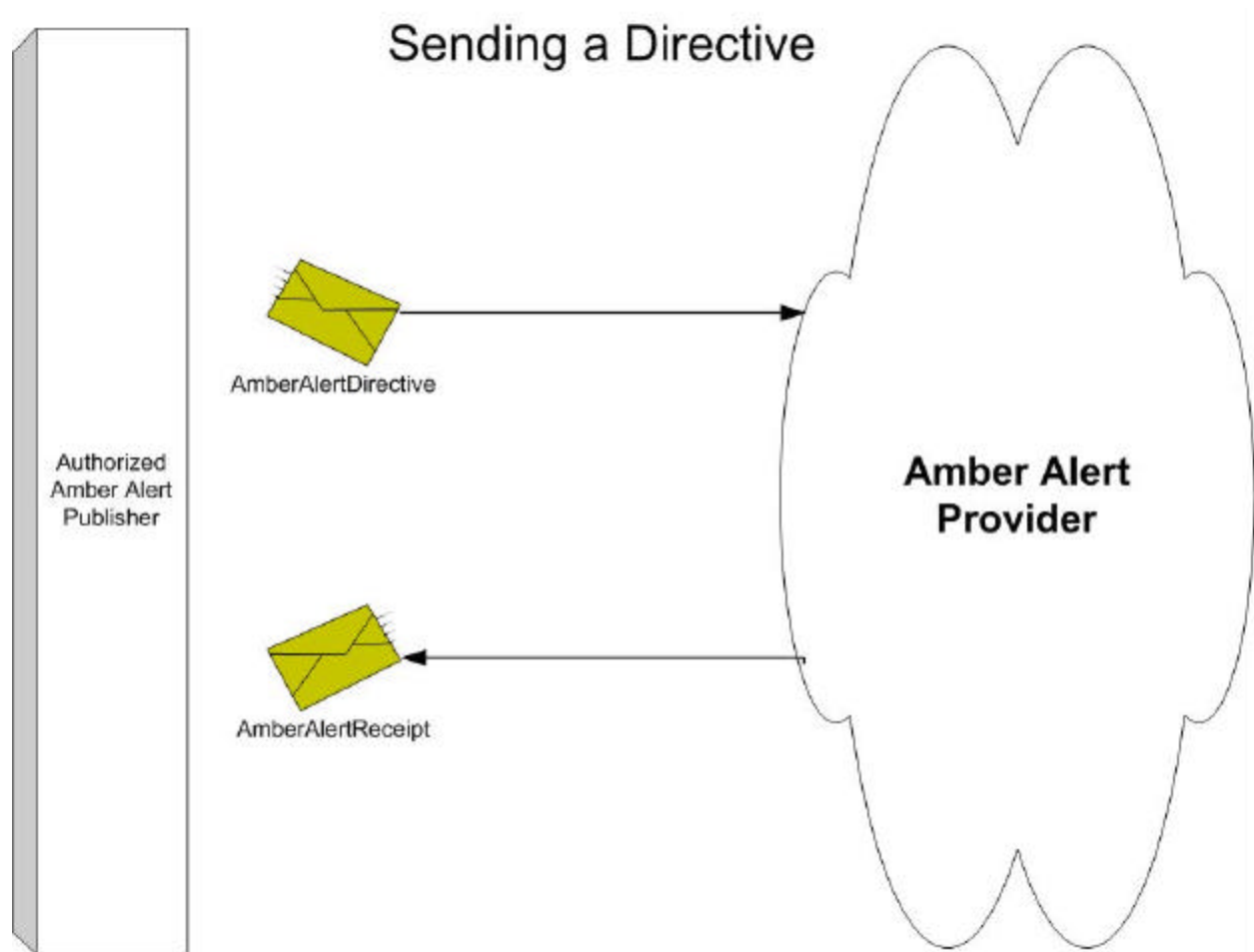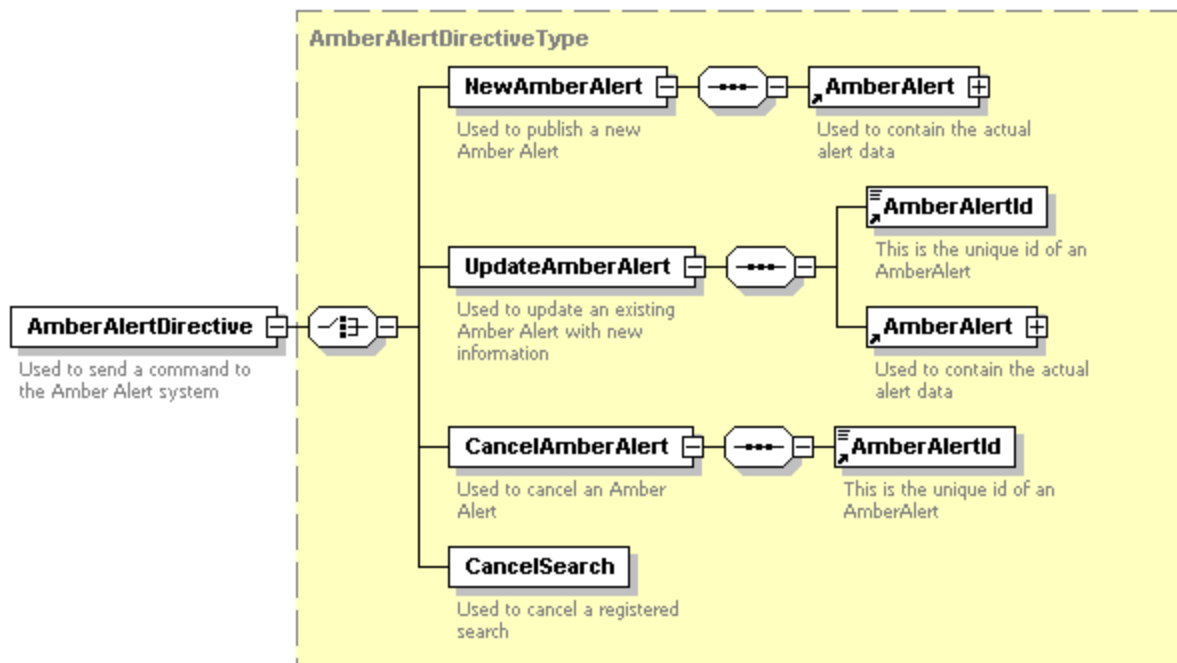**Figure 2-1: Sending an AmberAlert Directive**

Figure 2-2: AmberAlertDirective Details

2.2   Retrieving Amber Alerts

As shown in Figure 2-3, there are two ways to retrieve an Amber Alert from the provider. Initially, a requestor sends an AmberAlertSearch XML message to the provider. This message contains the criteria to be used for the search. The provider will respond with an AmberAlertResponse XML message. This message will contain between zero and n AmberAlert messages representing the results of the search request. Additionally, this message can request that these particular criteria be saved for future searches.

A second way to retrieve Amber Alerts from the provider is to request new results from a saved search. In this case the requestor sends an AmberAlertGet XML message to the provider. The provider will again respond with an AmberAlertResponse XML message. The AmberAlertResponse message will contain AmberAlert messages for all new Amber Alerts matching the criteria set up by a previously saved search.
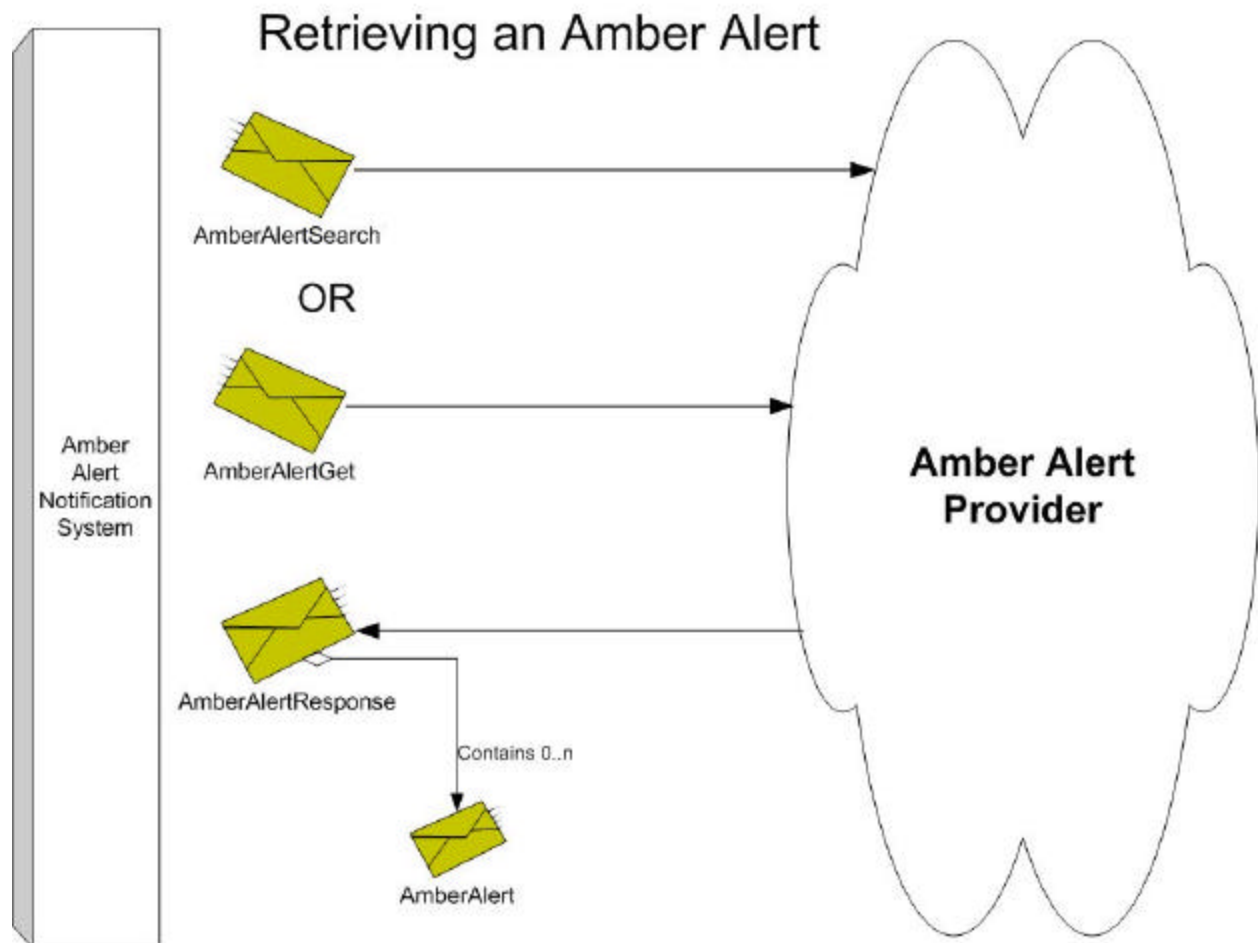
Figure 2-3: Retrieving an Amber Alert

2.3   Amber Alert Message Types

Figure 2-4 provides an overview of the message types present in the proposed message framework. The messages are placed in one of three classifications: Primary Actions, Primary Data, and Responses. Primary Actions are the things that the system can be asked to do, such as search for Amber Alerts. Primary Data is the real data with which the system is primarily concerned, in this case Amber Alerts. Responses indicate all of the possible responses to a Primary Action.
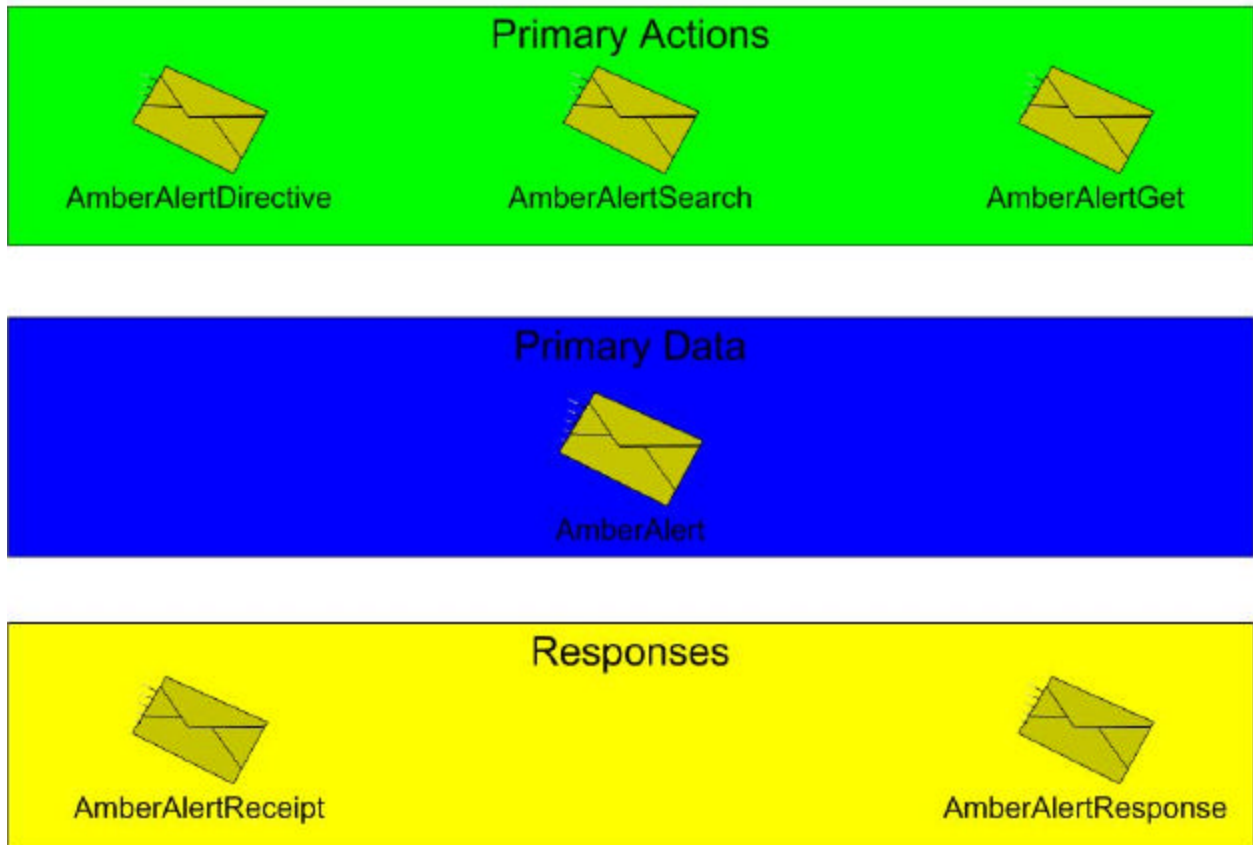
Figure 2-4: Amber Alert Message Types

3   Future Considerations

We recognize that the creation of an Amber Alert XML specification does not solve all of the existing problems with Amber Alerts. The list below highlights some of the problems that remain to be solved. This list was compiled based on our research and information provided by state and local law enforcement agencies, along with NCMEC and the FBI.

- Standardization of Amber Alert criteria among various agencies

- Consistent, timely, entry of information into NCIC and VICAP

- Standardized process for sharing Amber Alerts across agencies / regions

In order to begin to address these problems, a centralized repository of Amber Alert data should be investigated. This centralized repository would not replace the existing Amber Alert providers. Instead, this repository could facilitate some high level management of the Amber Alert process and data in an attempt to address some of the shortcomings of the existing process.

Appendix A: Schema Diagrams
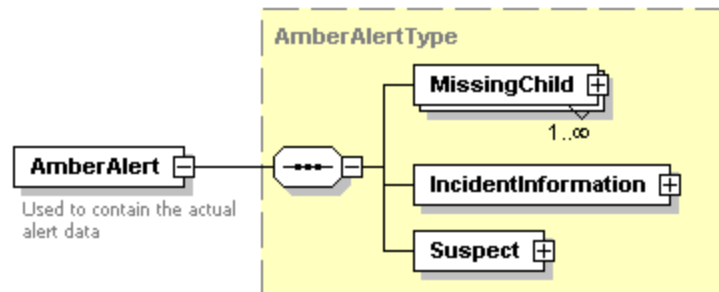
Figure A-1: AmberAlert
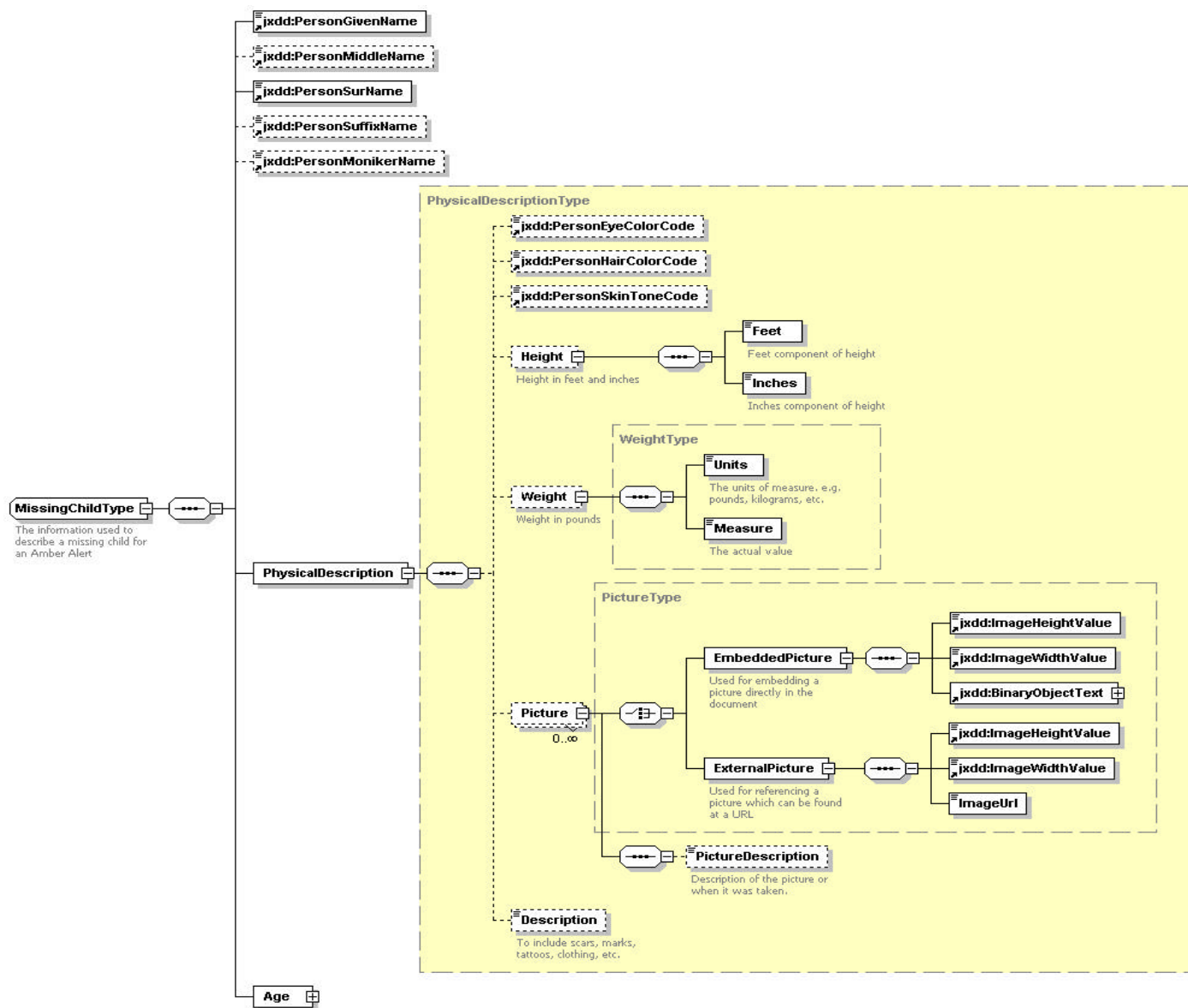
Figure A-2: MissingChildType
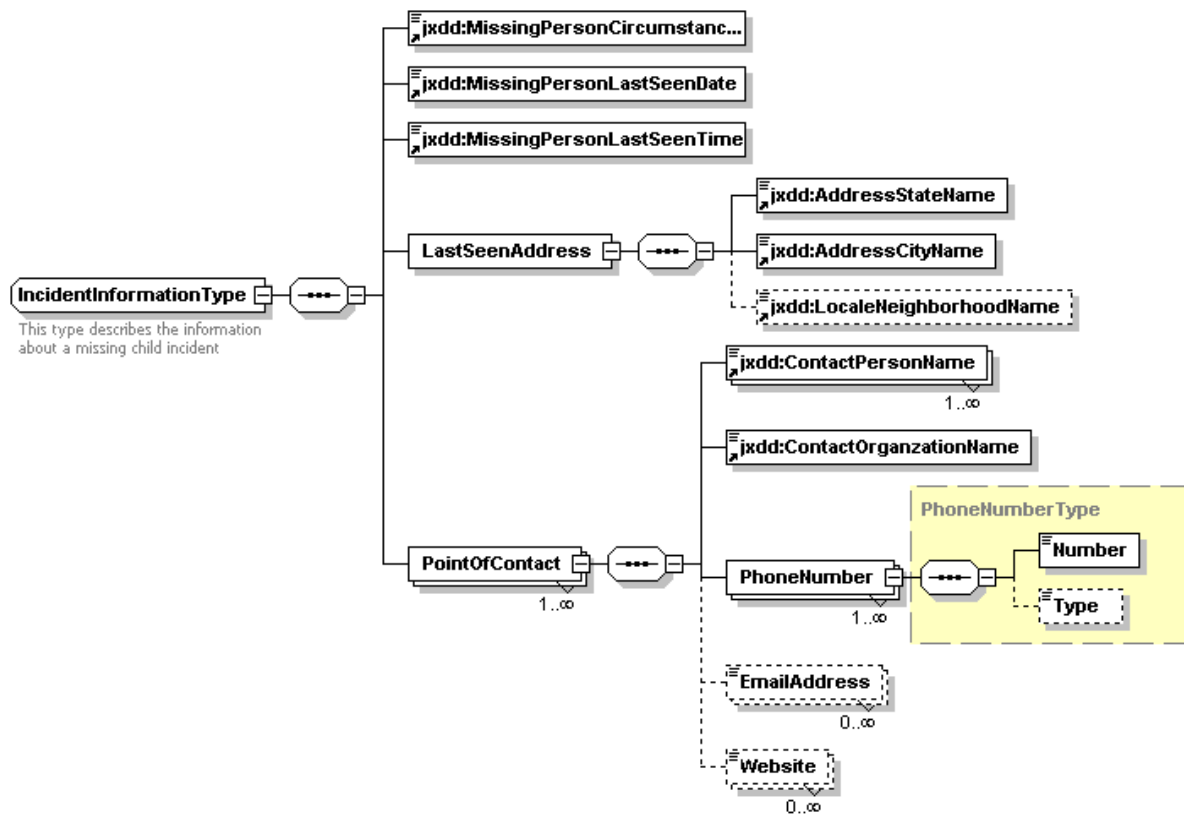
Figure A-3: IncidentInformationType
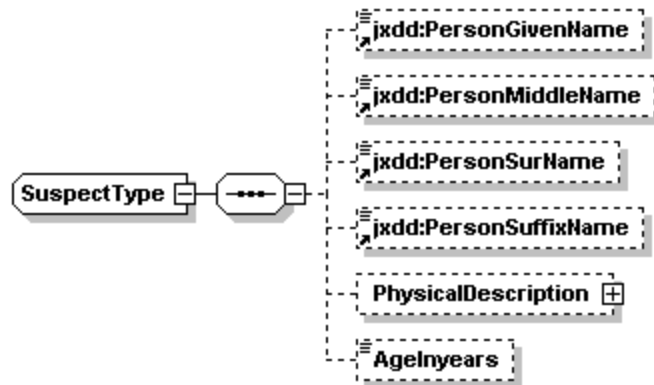
Figure A-4: SuspectType
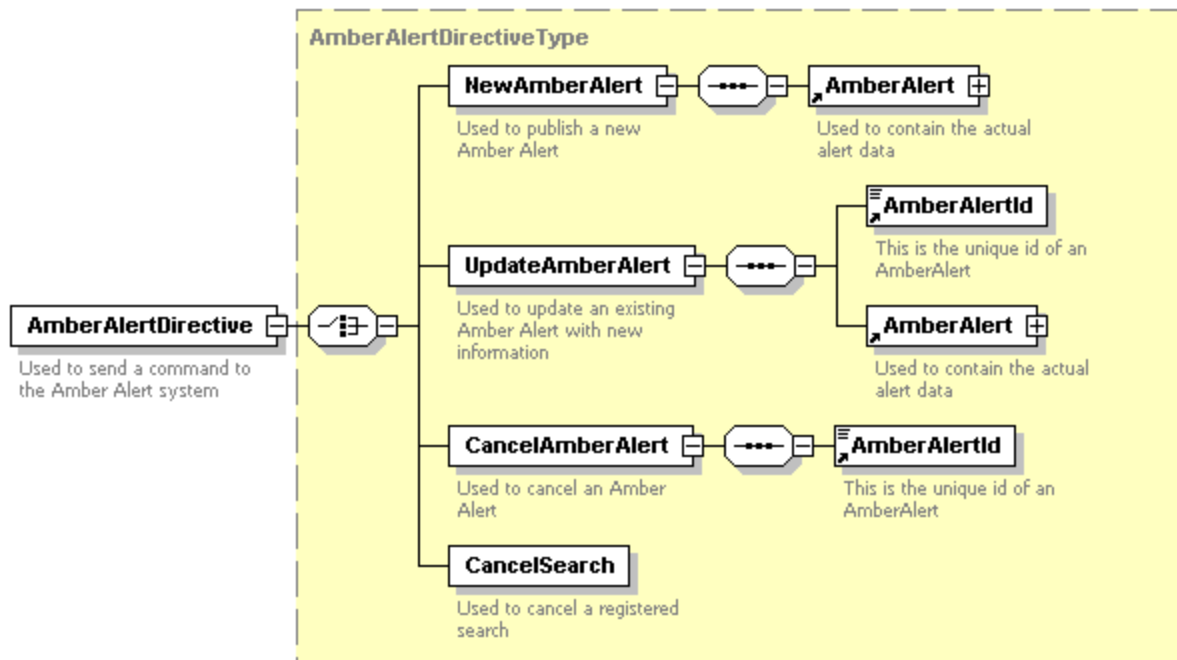
Figure A-5: AmberAlertDirective
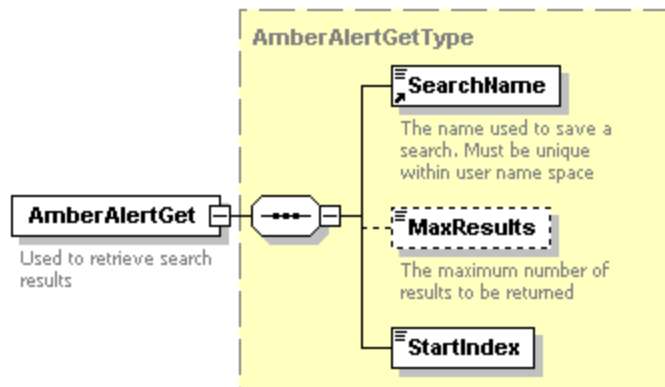
Figure A-6: AmberAlertGet
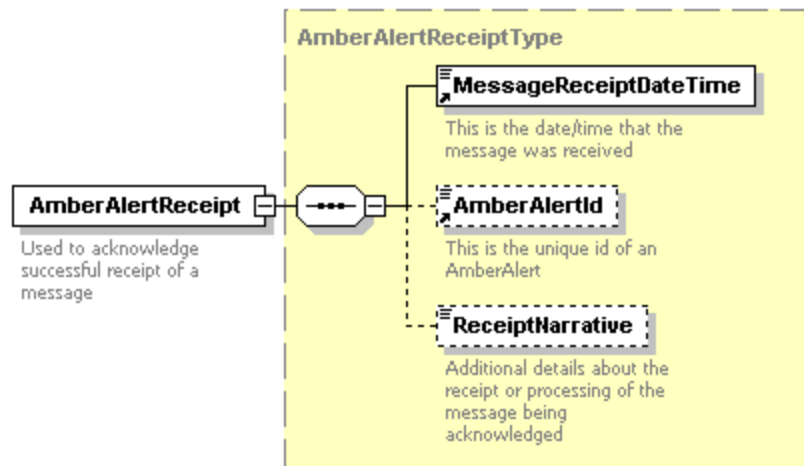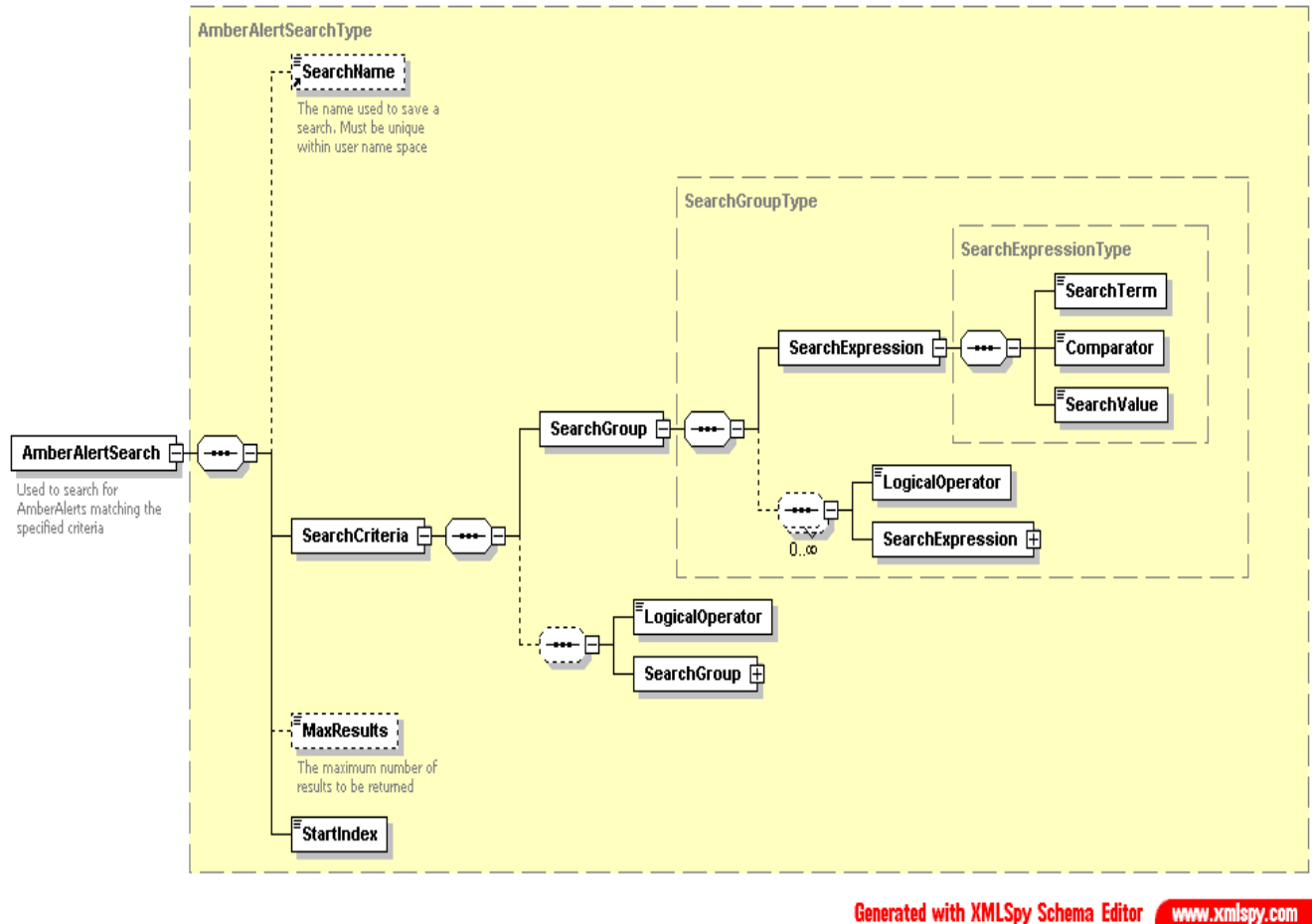
Figure A-7: AmberAlertReceipt
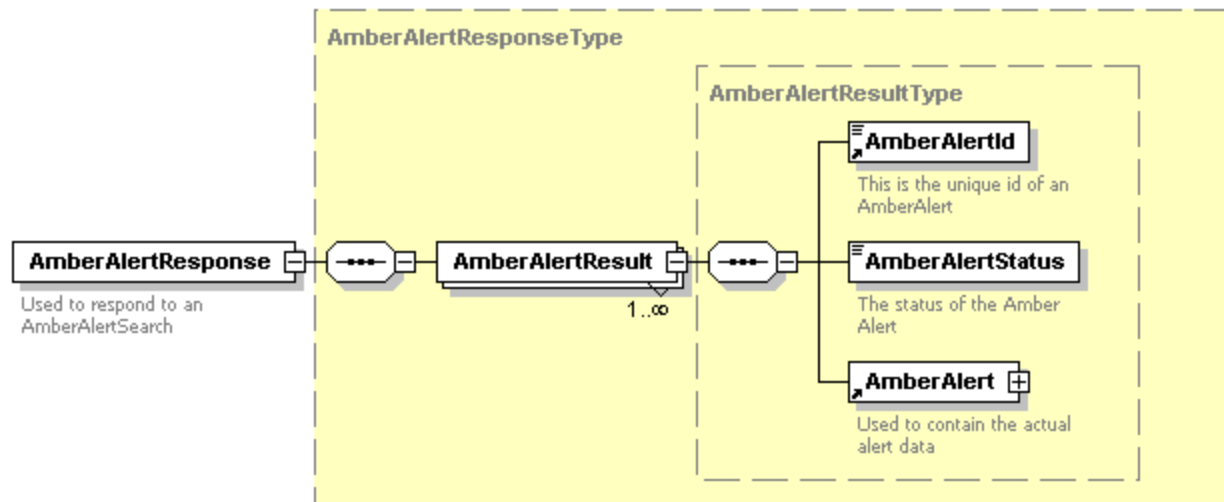
Figure A-8: AmberAlertResponse

Figure A-9: AmberAlertSearch